Appendix 3: AED Guidelines for Data Security

AED Data Security Policy

All personnel from the Academy for Educational Development and their contractors will adhere to the following procedures to ensure security for confidential data.

a. Documentation of Pledge to Confidentiality:
Any persons using or handling confidential data will sign confidentiality pledges asserting that they will adhere to the guidelines for confidential data use and nondisclosure.

b. Restriction of Personnel with Access:
The Principal Investigator (PI) will identify personnel with a "need to know" who are allowed access to confidential data. Staff members affiliated with a project (including the relevant members of IT staff, system administrators, and contractors) must sign confidentiality pledges for that project. Access to confidential data will be denied to anyone without a documented need and signed confidentiality pledge.

c. Secure Delivery Mechanisms for Data:
All data containing confidential information will be transferred to AED for analysis using a secure FTP site from via secure mail from GroupWise. *Inappropriate Delivery Mechanisms for Data include d*ialup from home computers (confidential data should not be on home computers in the first place), and unencrypted file transfer over the Internet (examples: ftp, transfer via terminal emulator) to any AED site computer.

d. Confidential Password Management:
Passwords that give access to confidential data are themselves confidential data and will be handled as such for all purposes. Specific password guidelines follow:

- Do not share your password with anyone.
- Do not use easily guessed passwords.
- The most effective passwords contain a mix of uppercase and lowercase letters, and
- At least one number and special character.
- Never select a password that is completely numeric.
- Choose long passwords. Acronyms created from phrases you can remember are a good approach,
- Do not write down your password. Pick a password you can remember instead of one you'd have to write down.

If you think your password has been compromised, change it immediately and report the situation as soon as possible to the data security officer.

e. Confidential Computer Sessions:
AED researchers using an account or a computer with access to confidential data will not leave the session unattended. They will log out, and lock up any storage media that hold confidential data.

f. Labeling of Confidential Storage Media:
Storage media (diskettes, tape cartridges, CDs, internal and external hard drives) that hold confidential data will be labeled with the following information:

- The word “CONFIDENTIAL”
- Tracking number

g. Logging:
PIs or their designated assistants will keep a paper log for each piece of confidential storage media (CD, diskette, tape cartridge, internal or external hard drive) showing what happens to the item while it is in their care.

- Log the following events:
- Receipt of item from external source
- Destruction of item
- Transfer of item to someone else's responsibility (even within the Partner site)

Log will include:

- Date
- Name
- Description (what happened, to whom transferred, etc.)

h. Removal of Confidential Storage Media or Printouts:
Confidential storage media and printouts can be removed from AED secure holdings only if it is physically handed to a person authorized to receive it. This transfer must be logged.

i. Identification:
As confirmed in the confidentiality pledge, researchers will not attempt to identify individuals, families, or households. If identification inadvertently occurs, researchers will make no use of the information, safeguard the information, and not inform anyone else of the discovery. Researchers will never report results in a way that could permit inadvertent disclosure of an individual. When tabulations are produced, any table with a cell of 1, 2, or 3 cases will be re-categorized, if necessary.

j. Printing:
Confidential printouts containing individual information will not be printed. Any other printouts of aggregated information will be stored safely at all times. The PI or their designated assistant will be responsible for data print-outs and keep them in a locked file cabinet. As a result, researchers will not send confidential data to any "public" printers (where any passerby can see or take the printouts), unless researchers can be with the printer while it is printing. Note that it is not necessary to log what happens to printouts that never leave secured premises.

k. Disposal or Scrubbing of Confidential Storage Media:
AED will destroy any confidential data held on site by physically destroying any CD’s and erasing it off mobile drives. All data on site will be permanently destroyed at the completion of the project. Paper copies of completed surveys and interview and focus

group transcripts will be secured in a locked cabinet for the required time, after which they will be shredded.

l. Backups:

Note that backups of confidential data are themselves confidential, and require logging. An external agency might require special practices for locking up backup media.

- Backups will be encrypted if they contain confidential data.
- Backup tapes, diskettes or CDs containing confidential data will be kept in secured areas or cabinets.
- Backup tapes, diskettes, or CDs containing confidential data will be sanitized before they are discarded or disposed of according to the guidelines in the section on disposal of confidential storage media.

m. Periodic Review of Confidential Holdings:

PIs are responsible for training and reviewing the proper handling of confidential data with their staff. PIs will conduct a semi-annual review of confidential logs, confirming that all confidential media can be accounted for.